# Department of Justice

STATEMENT

OF

ROBERT S. LITT

DEPUTY ASSISTANT ATTORNEY GENERAL

CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE

AND CONSUMER PROTECTION

COMMITTEE ON COMMERCE

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

CELLULAR PHONE PRIVACY

PRESENTED ON

FEBRUARY 5, 1997

REMARKS OF DEPUTY ASSISTANT ATTORNEY GENERAL
ROBERT S. LITT
HOUSE COMMERCE COMMITTEE
SUBCOMMITTEE ON TELECOMMUNICATIONS

HEARING ON CELLULAR PHONE PRIVACY

Washington, D.C.
February 5, 1997

Mr. Chairman, members of the Subcommittee, I would like to thank you for inviting me to be with you today. I greatly appreciate the opportunity to present the views of the Department of Justice on cellular telephone privacy.

I would like to begin with an important principle chat I believe everyone can agree upon. No one engaged in legal activities should have to fear that his or her telephone conversations are being surreptitiously listened to by others. Even when you are using a cellular phone, you have the right to expect that your conversations with your family, your friends or yaur business associates are only between you, and arc not exposed to the whole world. To ensure that private conversations remain private, we need to rely upon both technical solutions and legal protections. 'The Department of Justice has been doing, and will continue to do, its part in protecting the privacy of communications.

The Statutory Framework

The principal federal law protecting the privacy of telephone communications is Title III of the Omnibus Crime Control and Safe Street Act of 1968, which is codified as amended at Sections 2510 to 2521 of Title 18 of the united States Code.

Title III generally forbids the intentional interception of any wire, oral or electronic communication without the consent of a party to the conversation.[1] The statute also forbids the intentional disclosure or use of the contents of any wire, oral or electronic communication if you know or have reason to know that the information war obtained through an illegal interception.[2]

Any person who intercepts or discloses a communication in violation of Title III is subject to criminal prosecution,[3] and may be civilly liable to any person whose communications are intercepted.[4] Those civil liabilities can include statutory damages of $10,000 or $100 a day (whichever is greater) or the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation.[5]

Ordinarily, a criminal violation of Title III is a felony, punishable by a maximum penalty of five years in jail and a fine of $250,000.[6] However, as you probably know, a cellular telephone conversation is transmitted in part by radio and in part over telephone wires. As originally enacted, Title III did not clearly cover the radio portion of cellular telephone

---

1 18 U.S.C. § 2511(1)(a).

2 18 U.S.C. § 2511(1)(c), (1)(d).

3 18 U.S.C. § 2511(4).

4 18 U.S.C. § 2520.

5 18 U.S.C. § 2520(c)(2).

6 18 U.S.C. § 2511(4)(a)

communications. In 1986, Title III was amended by the Electronic Communications Privacy Act("ECPA"), which, among other things, filled this gap. Today, therefore, it is illegal to intentionally intercept the radio portion of a cellular telephone conversation, or to disclose or use such an *intercepted* communication, knowing ox having reason to believe it was illegally intercepted.

It is Lhe radio portion of cellular phone calls -- that is, the transmission occurring between the cellular telephone and a radio tower -- that is the most vulnerable to interception. At the time ECPA was passed, and for a *number of years* thereafter, this radio portion could be intercepted by anyone with a police scanner. Because the technology made interceptions so simple, Congress determined that, unless there were aggravat isg circumstances, the interception, disclosure, or use of the radio portion of a cellular telephone communication should be treated as an infraction, the least serious category of federal criminal offense .[7] No term of imprisonment is authorized for thio infraction, and the maximum fine is $5,000.[8]

The interception, disclosure or use of the radio portion of a cellular telephone conversation can, however, be charged as a felony, If there are aggravating circumstances. Those

---

[7] 18 U.S.C. §§ 3559(a) (9); 3581(9).

[8] 18U.S.C.§§ 2511(4) (b) (ii); 3571(c) (7). The penalty under ECPA was increased in 1994 from $500 to $5,000. Section 3571(d) also provides for an alternative fine of twice the gross gain to the defendant or loss to the victim.

circumstances are: (i) if the violation is not a first offenra or (ii) if the act is done far tortious or illegal purposes (such a.6 blackmail) or for purposes of direct or indirect commercial advantage or private financial gain. In such a case, the offender can be imprisoned for no more than five years, fined up to $250,000, or both.

To prove a violation of Title III, the government must prove that the interception, disclosure, or uoe was intentional. As stated in the legislative history, "'[i]ntentional" means mare than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objecr ive."[9]

Ina case involving the disclosure or use of an illegally intercepted communication, the government must also show that the individual who disclosed or used the intercepted communication knew or had reason to *know* "that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection [of Title 1111."[10] This language does ncc permit a defendant to escape liability by claiming that he or she did not know what Title III prohibits. In other words, a defendant cannot claim he or she did not know thr law. Instead, the government must prove only that the defendant knew or had reason to know that the

---

[9] S. Rep. *No. 541,* 99th Cong., 2d Sess. 23, reprinted in 1586 U.S. Code Cong. & Admin. News 3555, 3557.

[10] 18 U.S.C. § 2511(1)(c),(d).

interception was made under circumstances which in fact violated Title III.

Most cellular telephones broadcast at a frequency between 800 and 900 megahertz, a range setaside by the Federal Communications Commission (FCC) for this type of use. As noted, for many years after the passage of ECPA, it was perfectly legal to manufacture or sell police scanners that were capable of intercepting communications broadcast within that frequency. In 1993, however, in response to a Congressional mandate, the FCC issued a regulation requiring that no publicly available police scanner manufactured in or imported into the United States after that April of 1994 (the regulation's effective date) should be able to intercept transmissions in the cellular frequency range. The regulation also requires that the scanners not he able to be readily altered by the user to pick up such frequencies,

Thus, while users of alder scanners can still pick up cellular telephone calls, users of newer scanners that comply with the FCC regulation -- including many individuals who enjoy listening to transmissions of emergency services -- are not able to intercept the transmissions of the radio portion of cellular telephone transmissions, and do not pose a threat to the privacy of cellular telephone users.

A greater threat to privacy is posed by individuals who modify their scanners so that they can intercept cellular telephone transmissions. Under Title III, the modification of a police scanner may 'constitute a felony violation if that scanner

is sent through the mail or transported in interstate or foreign commerce.[11]

Title III is not the only statute that may be implicated by the interception of cellular radio signals. Although rarely employed in these circumstances, section 705(a) of the Communications Act, 47 U.S.C. § 605(a), prohibits, among other things, tha unauthorized interception of any radio communication, and divulging the contents of the communication knowing it was improperly intercepted, and may be applicable to the radio portion of the cellular communications. Willful violations of Section 605(a) are punishable by imprisonment of up to six months, fines of not more than $2,000, or both.

Enforcement Efforts

The Justice Department has, in appropriate cases, prosecuted individuals for the improper interception, disclosure or use of communications. Justice Department statistics show that in tht last five years, almost 100 cases have been brought charging violations of 18 U.S.C. § 2511. However, we do not keep separate statistics identifying the particular type of communication that was illegally intercepted, and so we art unable to tell you how many of those cases involved cellular communications.

Technical and Legal Issues

To the extent that the radio portion of cellular communications can be easily intercepted, technical solutions may serve to best protect communications privacy by modifying readily

---

[11] 18 U.S.C. § 2512.

available devices. For example, the cellular telephone industry is developing products and protocols that rely upon robust encryption to protect the radio portion of cellular communications. The Department of Justice supports these efforts as an important step towards preserving privacy, as long as these technologies are implemented in a way that preserves law enforcement access to the unencrypted communication when legally authorized.

The Department will also investigate and prosecute the illegal interception or disclosure of cellular calls, although we must consider, when establishing investigative priorities, that Congress has seen fit to treat such offenses as infractions, Certainly, in circumstances when the crime may be a felony -- either because it is a second or subsequent offense, or because the interception, disclosure, or use was committed for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private financial gain -- that fact will be considered in determining whether the case should be pursued.

However, the Subcommittee may wish to explore whether It continua to make sense to attach significantly different penalties to illegal interception of a telephone conversation depending on whether it was the radio or non-radio portion of the contents of a cellular telephone call that was intercepted or disclosed. From the point of view of the person having the conversation, the invasion of privacy is the same: If the

Subcommittee wants to consider this issue, we would be pleased to work with your Staff.

I would be happy at this time to answer any questions.